Tivoli Identity Manager

End User Guide

Version 4.5.1

SC32-1152-02

Tivoli Identity Manager

End User Guide

Version 4.5.1

SC32-1152-02

NOTE:

Before using this information and the product it supports, read the information in "Notices" on page 37.

Third Edition (February 2004)

This edition applies to version 4.5.1 of Tivoli Identity Manager and to all subsequent releases and modifications until otherwise indicated in new editions.

This edition replaces SC32-1152-01

© Copyright International Business Machines Corporation 2004. All rights reserved.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Preface v
Who Should Read This Book v
Publications v
Tivoli Identity Manager Server library v
Related publications vi
Accessing Publications Online vi
Accessibility vii
Contacting software support vii
Conventions used in this book vii
Operating System Differences viii
Revision Bars used in the Version 4.5.1 Library viii
Definitions for HOME Directory Variables viii

Chapter 1. Introduction 1
Tivoli Identity Manager Structure 1
Navigation 2
Organization Management 3
Person Management 3
Managing Services 3
Provisioning 3

Chapter 2. Logging In 5
Language Selector 5
Retrieving New Passwords 5
Forgotten Passwords (Password Challenge/Response) 6
Forced Challenge/Response Configuration 6
Retrieving a Password 7
Forced Password Change 7
Password Administration 7
Logging Out 7

Chapter 3. Common Features 9
Navigation 9
Main Menu Navigation Bar 9
Task Bar 9
Effective Date 10
Help 10

Chapter 4. Home 11
Password Management 11
Account Management 13
Adding New Accounts 14
Modifying Existing Accounts 14
Suspending or Deprovisioning Accounts 15
Restoring Accounts 15
Changing Passwords 15
To Do List 16
Viewing To Do List Request Details 18
Requests 18
Pending Requests 20
Completed Requests 20
Transaction Audits 20
Personal Information 21
Delegating Authority 22

© Copyright IBM Corp. 2004

Adding a Delegate 22
Changing the Delegate 22
Modifying the Selected Delegate 23
Password Challenge/Response Answers 23

Chapter 5. Reports 25
Report Types 26
Operation Report 27
Service Report 29
User Report 31
Rejected Report 32
Reconciliation Report 33
Dormant Report 34
Account Reports 35
Custom Reports 36

Notices 37
Trademarks 38

Glossary 41

Index 45

Preface

The IBM® Tivoli® Identity Manager Server (Tivoli Identity Manager Server) is an administrative tool to manage security across your entire organization. This manual describes how to use Tivoli Identity Manager end user functions and features.

Who Should Read This Book

This manual is intended for end users responsible for maintaining their Tivoli Identity Manager accounts. Readers are expected to understand basic Web and browser concepts and should be capable of performing routine end user tasks.

Publications

Read the descriptions of the Tivoli Identity Manager library, the prerequisite publications, and the related publications to determine which publications you might find helpful. After you determine the publications you need, refer to the instructions for accessing publications online.

Tivoli Identity Manager Server library

The publications in the Tivoli Identity Manager technical documentation library are organized into the following categories:

- Release Information
- Online User Assistance
- Server Installation
- Administration and Configuration
- Technical Supplements
- Agent Installation Information

Release Information:

- *IBM Tivoli Identity Manager Release Notes*

  Provides software and hardware requirements for Tivoli Identity Manager, and additional fix, patch, and other support information.
- *Tivoli Identity Manager Read This First Card*

Online User Assistance:

- Online user assistance for Tivoli Identity Manager

  Provides integrated online help topics for all Tivoli Identity Manager administrative tasks.

Server Installation:

- *IBM Tivoli Identity Manager Server Installation Guide on UNIX and Linux using WebSphere*

  Provides installation information for Tivoli Identity Manager.
- *IBM Tivoli Identity Manager Server Installation Guide on Windows using WebSphere*

  Provides installation information for Tivoli Identity Manager.
- *IBM Tivoli Identity Manager Server Installation Guide on UNIX using WebLogic*

© Copyright IBM Corp. 2004

Provides installation information for Tivoli Identity Manager.

- *IBM Tivoli Identity Manager Server Installation Guide on Windows 2000 using WebLogic*

  Provides installation information for Tivoli Identity Manager.

Administration and Configuration:

- *IBM Tivoli Identity Manager Policy and Organization Administration Guide*

  Provides topics for Tivoli Identity Manager administrative tasks.
- *IBM Tivoli Identity Manager End User Guide*

  Provides beginning user information for Tivoli Identity Manager.
- *IBM Tivoli Identity Manager Configuration Guide*

  Provides configuration information for single-server and cluster Tivoli Identity Manager configurations.

Technical Supplements:

- *IBM Tivoli Identity Manager Problem Determination Guide*

  Provides additional problem solving information for the Tivoli Identity Manager product.

Agent Installation:

- The Tivoli Identity Manager technical documentation library also includes an evolving set of platform-specific installation documents for the Agent component of a Tivoli Identity Manager implementation.

Related publications

Information related to Tivoli Identity Manager is available in the following publications:

- The Tivoli Software Library provides a variety of Tivoli publications such as white papers, datasheets, demonstrations, redbooks, and announcement letters. The Tivoli Software Library is available on the Web at:

  http://www.ibm.com/software/tivoli/library/
- The *Tivoli Software Glossary* includes definitions for many of the technical terms related to Tivoli software. The *Tivoli Software Glossary* is available, in English only, from the **Glossary** link on the left side of the Tivoli Software Library Web page

  http://www.ibm.com/software/tivoli/library/

Accessing Publications Online

The publications for this product are available online in Portable Document Format (PDF) or Hypertext Markup Language (HTML) format, or both in the Tivoli Software Library:

http://www.ibm.com/software/tivoli/library/

To locate product publications in the library, click the **Product manuals** link on the left side of the Library page. Then, locate and click the name of the product on the Tivoli Software Information Center page.

Product publications include release notes, installation guides, user's guides, administrator's guides, and developer's references.

Note: To ensure proper printing of PDF publications, select the **Fit to page** check box in the Adobe Acrobat Print window (which is available when you click **File > Print**).

Accessibility

The product documentation includes the following features to aid accessibility:

- Documentation is available in both HTML and PDF formats to give the maximum opportunity for users to apply screen-reader software.
- All images in the documentation are provided with alternative text so that users with vision impairments can understand the contents of the images.

Contacting software support

Before contacting IBM Tivoli Software support with a problem, refer to the IBM Tivoli Software support Web site by clicking the **Tivoli support** link at the following address:

http://www.ibm.com/software/sysmgmt/products/support/

If you need additional help, contact software support by using the methods described in the *IBM Software Support Guide* at the following Web site:

http://techsupport.services.ibm.com/guides/handbook.html

The guide provides the following information:

- Registration and eligibility requirements for receiving support
- Telephone numbers and e-mail addresses, depending on the country in which you are located
- A list of information you should gather before contacting customer support

Conventions used in this book

This reference uses several conventions for special terms and actions and for operating system-dependent commands and paths.

The following typeface conventions are used in this book:

Bold Lowercase commands or mixed case commands that are difficult to distinguish from surrounding text, keywords, parameters, options, names of Java classes, and objects are in **bold**.

Italic Variables, titles of publications, and special words or phrases that are emphasized are in *italic*.

`Monospace`
Code examples, command lines, screen output, file and directory names that are difficult to distinguish from surrounding text, system messages, text that the user must type, and values for arguments or command options are in `monospace`.

Operating System Differences

This book uses the UNIX convention for specifying environment variables and or directory notation. When using the Windows command line, replace *$variable* with *%variable%* for environment variables and replace each forward slash (/) with a backslash (\) in directory paths. If you are using the bash shell on a Windows system, you can use the UNIX conventions.

Revision Bars used in the Version 4.5.1 Library

The Tivoli Identity Manager version 4.5.1 technical documentation library makes use of revision bar characters to indicate where technical changes have occurred to the information previously found in the version 4.5 library. Revision bars are indicated by a vertical line (|) in the page margin to the left of the change.

Definitions for HOME Directory Variables

The following table contains the default definitions used in this document to represent the ″HOME″ directory level for various product installation paths. You can customize the installation directory and HOME directory for your specific implementation. If this is the case, you need to make the appropriate substitution for the definition of each variable represented in this table.

Path Variable	Default Definition

ITIM_HOME	**Windows:**
	`c:\itim45\`
	UNIX:
	`/itim45/`

WAS_HOME	**Windows:**
	`c:\Program Files\WebSphere\AppServer\`
	UNIX:
	`/opt/WebSphere/DeploymentManager/`

WAS_NDM_HOME	**Windows:**
	`C:\Program Files\WebSphere\DeploymentManager\`
	UNIX:
	`/opt/WebSphere/DeploymentManager/`

BEA_HOME	**Windows:**
	`c:\bea\`
	UNIX:
	`/usr/local/bea/`

Chapter 1. Introduction

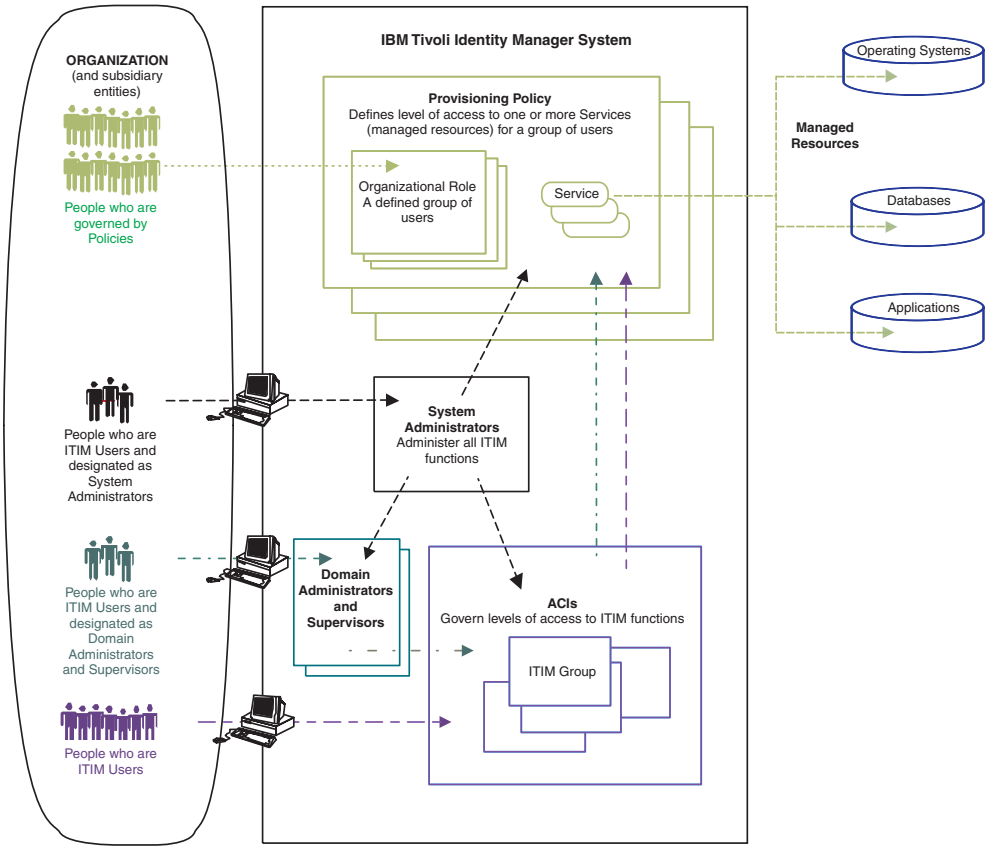
IBM Tivoli Identity Manager provides the software and services needed for deploying policy-based provisioning solutions. Tivoli Identity Manager helps companies automate the process of provisioning employees, contractors and business partners with access rights to the applications they need, whether in a closed enterprise environment or across a virtual or extended enterprise.

After organizations and subsidiary entities such as organizational units, business partner organizations, and locations are set up, person entities are added. Organization roles and ITIM groups can be created. Person entities can then be assigned to organization roles and ITIM groups. This process is continued by creating services, which allow access to the different types of managed resources such as Oracle, Windows NT®, and so on. Organization roles can be linked through provisioning policies and are linked to services, to allow the person entities in the various organization roles to access the managed resource that is linked to that service. ITIM groups, which allow access to the Tivoli Identity Manager Server, are granted rights within Tivoli Identity Manager by the use of ACI, and person entities are assigned to ITIM groups to allow the use of granted rights.

Tivoli Identity Manager Structure

The following is a basic overview of how the Tivoli Identity Manager system works.

© Copyright IBM Corp. 2004


ORGANIZATION
(and subsidiary entities)
People who are governed by Policies
IBM Tivoli Identity Manager System
Provisioning Policy
Defines level of access to one or more Services (managed resources) for a group of users
Organizational Role
A defined group of users
Service
Managed Resources
Operating Systems
Databases
Applications
People who are ITIM Users and designated as System Administrators
System Administrators
Administer all ITIM functions
People who are ITIM Users and designated as Domain Administrators and Supervisors
Domain Administrators and Supervisors
ACIs
Govern levels of access to ITIM functions
ITIM Group
People who are ITIM Users

Person entities are added to organizations and entities that are subsidiaries to an organization.

A person entity can be assigned to an organizational role, which confers access to managed resources through a provisioning policy. The policy sets the rights a person has when accessing the target managed resource.

An ITIM user is a person entity that has been provisioned with a Tivoli Identity Manager account. An ITIM user can also be assigned to an ITIM group, which confers access to the Tivoli Identity Manager Server, through the functions granted by an ACI.

Some person entities, usually only one or a few, are assigned as system administrators, and have access to all Tivoli Identity Manager functions, at all levels.

Navigation

The Main Menu Navigation Bar at the top of each page allows for easy navigation through the Tivoli Identity Manager system. You can then access functions within each Main Menu Navigation Bar selection by using the task bar choices on the left side of the system page.

The Tivoli Identity Manager system consists of one or more organizations that can contain subsidiary entities, such as organizational units, locations, and business partner organizations, all in a parent-child relationship. Each Tivoli Identity Manager entity can contain person entities, which can then be assigned to ITIM

groups and organizational roles. The role of system administrator can be assigned to person entities who need full access to all functional areas of Tivoli Identity Manager.

Organization Management

Organization management is performed using the My Organization tab on the Main Menu Navigation Bar. Clicking **My Organization** displays the Organization task bar on the left side of the page. The task bar displays functions performed within the organizations and their subsidiary entities, as well as the person entities contained within the organizations and other entities.

Clicking on My Organization, Tivoli Identity Manager displays a two-pane page. The left pane displays a list of the organizations, in a format that can be expanded/collapsed to show subsidiary entities. This list is used to select an entity. The right pane displays a list of entities (Organization, Location, Organizational Unit, Business Partner Organization) or Person (for the selected entity).

Any of the subsidiary entities can be subsidiaries of an organization entity or of any of the other entities. There is no restriction on hierarchy for subsidiary entities, so, for example, a location entity can contain other location entities, and an organization unit entity can contain other organization unit entities, along with any of the other subsidiary entities. An organization entity must always be at the top of the organizational hierarchy.

Person Management

Adding a person entity puts the entity into either an organization or other container such as an organizational unit, business partner organization, admin domain, or location entity. After a person entity is added to an organization or other container, that person entity can be provisioned with a service which allows access a managed resource, including the Tivoli Identity Manager Server.

Managing Services

Administrators can add a service to an organization, which opens the ability for person entities to access that service. A service is a managed resource, such as a Windows NT® Server, MS Exchange Server, or even the Tivoli Identity Manager Server. The term for allowing access to a managed resource is *provisioning*. Because the Tivoli Identity Manager Server is also one of the services that can be managed, there will be individuals who need that service provisioned, even if only to access and manage their own Tivoli Identity Manager accounts and personal information. If person entities are not provisioned to the ITIM Service, they have no access to any of their own information in Tivoli Identity Manager. If a person entity has services provisioned, that individual has access to those services.

Provisioning

Services are not provisioned to person entities, only to organizational roles. If an individual needs access to a particular service, that person entity must be assigned to an organizational role that is provisioned with that service.

Individuals who are to act as users of Tivoli Identity Manager can do so only through assignment to an ITIM group. ITIM groups are granted various types of access through Access Control Information (ACI) routines. An Access Control Information routine defines three things:

- Types of functions that are granted to the ITIM group
- Organization or subsidiary entity types upon which the granted functions may be performed
- Level within the organizational hierarchy at which the granted functions may be performed

Chapter 2. Logging In

The Log In routine keeps unauthorized users from accessing your Tivoli Identity Manager system, allows you to access the areas to which you have been authorized, and presents a forgotten password procedure if you cannot remember your password.

To log into Tivoli Identity Manager, you must enter your user ID and password. Your account is provisioned with the rights required to complete your duties. Your password must conform to the password rules for your organization.

To log in to Tivoli Identity Manager:

1. Enter your User ID and click Tab to move to the Password field.
2. Enter your Password and either press **Enter** or click **Login**.

Language Selector

Tivoli Identity Manager allows users to select the language used within the Tivoli Identity Manager system.

To change languages:

1. Click **Select Another Language** in the lower left corner of the login page.

   The Language Selector page opens.
2. Click the desired language.

   Tivoli Identity Manager Server is configured to use the selected language and the Login page reappears.
3. Log into the system and use as desired.

If you log on using the single sign-on capability and need to select a language, append `/language` to the Web site address. For example, enter:

`https://mysite.myco.com/itim/enrole/language`

For more information on configuring the language default for your Web browser, refer to the *Tivoli Identity Manager Server Configuration Guide*.

Retrieving New Passwords

After a new account has been added to a user, the system will notify the user through e-mail, using the e-mail address in the personal information record. The system can be configured so the user receives an e-mail that contains the account password in clear text, or a URL and transaction ID number. If the administrator has configured Tivoli Identity Manager to disallow the emailing of passwords, you may have to see your supervisor in order to retrieve your new password.

The following procedures describe how to retrieve a new password using the URL and the transaction ID. The user must be able to provide the shared secret to retrieve the new password.

To retrieve a new password:

1. Click the URL shown in the e-mail to display the Retrieve Password page.

© Copyright IBM Corp. 2004

The Retrieve Password page opens with the Transaction ID field filled with the Transaction ID number that was provided in the e-mail.

2. Type the shared secret in the Shared Secret text field and click **Submit**.

   The Password Retrieval page opens.

3. Make a note of the password and click **Done**.

   The Password Retrieval page closes.

   Important: Make sure to write the password down, as this page will no longer be available.

Forgotten Passwords (Password Challenge/Response)

If a user forgets a password, the user can still log in to the system by answering the Password Challenge/Response questions correctly. After the user answers the challenge/response questions, Tivoli Identity Manager responds in one of the following manners, depending on the configuration of the system:

- The user is logged in to the system and is forced to change the password immediately.
- The user is e-mailed a new password in plain text.
- The user is e-mailed a link to retrieve the new password using the shared secret.

To log in using the Password Challenge/Response feature:

1. Type the login name in the Login Name field.
2. Click the **Forgot your password?** link on the login page.

   Note: If the Password Challenge/Response feature is disabled, the following message appears:

   ```
   Password challenge/response is currently disabled.
   Please contact your Identity Manager system administrator
   for more information.
   ```

3. Answer the challenge/response questions and click **Submit**.

   The system responds according to one of the system configurations described below:

   - The user is logged in to the system and is forced to change the password immediately.
   - The user is e-mailed a new password in plain text.
   - The user is e-mailed a link to retrieve the new password using the shared secret.

Forced Challenge/Response Configuration

The Password Challenge/Response feature, if enabled, allows a user access to the Tivoli Identity Manager system if the user forgot his password. If the Password Challenge/Response feature is disabled, the user is required to contact the system administrator for access to the Tivoli Identity Manager system.

Whenever the Password Challenge/Response feature is enabled for the first time or subsequently modified, users are required to set their responses to the Password Challenge/Response questions. Depending on the type of Challenge Mode, a user might need to define challenges and provide responses to the challenges, select challenges and provide responses to the selected challenges, or provide responses to the challenges presented.

Follow the prompts at the top of each page to configure the Password Challenge/Response feature.

Retrieving a Password

If the Tivoli Identity Manager Server is configured to e-mail the user a link to retrieve the new password, the user must be able to provide the shared secret to retrieve the new password.

To retrieve a password:

1. Click the URL shown in the e-mail to display the Retrieve Password page.

   The Retrieve Password page opens with the Transaction ID field filled with the Transaction ID number that was provided in the e-mail.
2. Type the shared secret in the Shared Secret text field and click **Submit**.

   The Password Retrieval page opens.
3. Make a note of the password and click **Done**.

   The Password Retrieval page closes.

   Important: Be sure to write the password down, as this page will no longer be available.

Important: You **must** log in and change your password immediately after retrieving the new password. After you click **Done**, the transaction ID is no longer valid and you will **not** be able to retrieve the new password again.

Forced Password Change

Users can be forced to change their password the first time they log in to the Tivoli Identity Manager Server system using a new account or the next time they log in using an existing account.

Note: This feature applies only to Tivoli Identity Manager accounts.

Users who are forced to change their password are taken to the `Enforce Password Change > Change Password` page immediately after logging in. The user cannot access any features in the Tivoli Identity Manager system until the password has been changed.

Password Administration

Password integrity is everyone's responsibility. Adhere to a policy of setting password lifetimes and changing passwords regularly. Do not store password information in areas accessible by others. Report suspected security violations and any changes in user status.

You should never give your password to another person, not even to those within your organization that are authorized to perform duties on your behalf. Tivoli Identity Manager provides delegation features in such cases.

Logging Out

To log out of Tivoli Identity Manager session, select the the Logout button located at the right-hand top corner of the Tivoli Identity Manager interface. You will be returned to the Tivoli Identity Manager Login page.

Chapter 3. Common Features

There are a few common features used throughout the Tivoli Identity Manager system. These features include the navigational features (Main Menu Navigation Bar and task bar), and the effective dates feature.

Navigation

The main features used to navigate through the Tivoli Identity Manager system are:

- Main Menu Navigation Bar
- Task bar
- Organization tree

See the following sections for more information about each navigation feature.

Main Menu Navigation Bar

The Main Menu Navigation Bar is located at the top of every page and has the following selections:

- Home
- Report
- Help

These selections allow users to quickly move to specific areas within the Tivoli Identity Manager system.

Note: The current location in the system is displayed on every page in the navigation path. The navigation path is prefaced with the phrase: `You are here:`

Task Bar

The task bar is located along the left side of every page of the Home, My Organization, Provisioning, and Report areas of the system and displays additional sub-areas for each topic area in the Main Menu Navigation Bar.

The following table shows what task bar options are available for each Main Menu Navigation Bar topic.

Main Menu Navigation Bar Topic	Task Bar Options
Home	Manage Passwords Manage Accounts Access To Do List View Pending Requests View Completed Requests Access Personal Information Delegate Authority Password Challenge Response

© Copyright IBM Corp. 2004

Main Menu Navigation Bar Topic	Task Bar Options
Report	Run Report Control Access Design Schema Design Report Synchronize Data
Help	*No task bar options available*

Effective Date

The effective date is the scheduled date and time an event occurs. You can select the exact date and time for the event or select the Schedule Immediately box to initiate the event immediately.

After making your selection, click **Submit** to process it. When the page returns to displaying the list of entities you have modified, you might need to click **Refresh** to update the page being viewed.

Help

The Help topic in the Main Menu Navigation Bar opens the online help for the Tivoli Identity Manager Server in a separate window. The online help provides information about concepts and features in the Tivoli Identity Manager system.

Each page also has a context-sensitive link to the online help. This link is the question mark button located in the top right corner of each page.

Chapter 4. Home

Home allows users to view and edit information that directly applies to themselves. Individuals who are granted access to view their own information can use the Home section to manage their personal information and action items.

The Home section allows users to:

- Manage passwords for their accounts
- Manage their accounts
- Access their To Do List
- View their pending and completed requests
- Access their personal information
- Delegate authority to other users
- Set their Password Challenge Response answers

See the corresponding sections for information about each task bar option.

Password Management

The password management section of Home is available through the Manage Passwords option in the Home task bar. This section allows users to manage all of the passwords to all of their accounts from one location.

Note: Always choose quality passwords that cannot be guessed easily. Passwords to avoid include names of family or common words found in the dictionary.

Passwords are subject to password policies created by an administrator. If password policies are implemented, passwords will adhere to the rules contained within the policy.

The Manage Password page has the following fields and features:

Field Name	Field Type	Description
New Password	Text field	Text field used to enter new password.
Confirm Password	Text field	Text field used to confirm password.
Create Password	Check box	Used to determine if system should generate a new password for the account. If this check box is selected, the system will generate a new password for the account and e-mail the address associated with the account the information necessary to retrieve the new password.
Effective Date selection field	Drop down menus Check box (Schedule immediately)	Selection fields to determine the time and date the new password will take effect. See “Effective Date” on page 10 for more information.

© Copyright IBM Corp. 2004

Field Name	Field Type	Description
Service Table	Text	Table that lists the services to which the user has accounts. The table has five columns. See the following table for more information about the Service table.
Submit	Button	Used to submit the changes to the system.
Reset	Button	Used to reset the values on the page to the last saved values in the system.
View Combined Password Rules	Hyper link	Opens a page that displays a combination of the password rules for all of the services listed.

The Services table lists the services to which the user has accounts. The following table describes each column in the Services table:

Column Name	Description
(check box)	If selected, the changes made apply to the account for the corresponding service.
Rules	This column has icons that link to the password rules for a specific service.
Service	Name of the service.
Login	User's login ID for the corresponding service.
Status	Status of the user's account.

To change your password:

1. Click **Home** in the Main Navigation Menu Bar.
2. Click **Managing Passwords** in the task bar.

   The Manage Password page opens.
3. Type a new password in the New Password Text field and confirm it in the Confirm Password text field **OR** select the Create Password check box.

   If Create Password is selected, Tivoli Identity Manager generates a password for the user and e-mails it to the address associated with the account.
4. Select an effective date and time **OR** select the Schedule Immediately check box.
5. Select the check boxes next to the services for which you want to change the password.
6. Verify that the password conforms to the password rules for the selected services by clicking the View icon next to the services.

   If a user is changing the password for more than one service, the user can click the **View Combined Password Rules** link to see the restrictive components of each set of password rules.
7. Click **Submit**.

   The changes are submitted and take effect when scheduled.

Account Management

The Account Management section of Home is available through the Manage Accounts option in the Home task bar. This section allows users to manage all of their accounts from a central location.

The Account Management page displays the following:

Column Name	Description
Check box	Selects the account listed in the row.
Compliancy Status	Specifies whether an account is compliant with current policies. See the table below for compliancy flags and descriptions.
User ID	User ID for each account.
Service Name	Service for which the account is used.
Status	Status of the account.

The Compliancy Status is indicated by one of four flags. Each flag has its own definition. The following table describes each of the compliancy flags.

Compliancy Status Flag	Description
	A blank graphic is used to indicate accounts that are compliant to the existing Provisioning Policies. This graphic can be modified to display a check mark or a green light. The name for this file is `acct_compliant.gif`.
	A question mark is used only for accounts returned from reconciliations. This flag indicates that policy checking was not performed during the reconciliation. All accounts returned from the reconciliation are marked with this flag.
	The warning sign indicates that an account is allowed to exist for the user but one or more of the account attributes do not compile with existing policies.
	The noncompliant sign indicates one of two scenarios: • The user is not allowed to have access to the specified resource and the account is not supposed to exist. • A Provisioning Policy is not defined for the resource.

The accounts can be sorted by User ID, Compliance, or Status.

Detailed information about an account is displayed by clicking the account's user ID. Any changes to the account can be scheduled to take effect immediately or be scheduled for a future time.

The Account Management page provides users with the option to perform the following:

- Add new accounts for existing services
- Modify existing accounts
- Suspend (inactivate) accounts
- Deprovision (delete) accounts
- Restore (reactivate) accounts
- Change passwords

Adding New Accounts

Authorized users can add new accounts to existing services for themselves.

To add a new account:

1. Click **Home** in the Main Menu Navigation Bar.
2. Click **Manage Accounts** in the task bar.

   The Account Management page opens.
3. Click **New**.

   The Provision Service page opens.
4. Select the radio button for the service for which you want to add a new account and click **Continue**.

   The Provision a New Service page opens. The fields displayed on this page are dependent on the type of service selected.
5. Fill in the applicable data on the screen.

   Note: If the Change Password at Next Logon? check box is selected, the user is required to change the password when first logging into the system.
6. Click **Submit**.

   The Enter Password and Select Effective Date | Time page opens.
7. Enter a password for the account and confirm it in the Confirm Password text field.

   Be sure to conform to password rules or the password will not be accepted.
8. Select an effective date and time and click **Submit**.

   See "Effective Date" on page 10 for more information.

   The request is submitted and the Account Management page reappears.
9. Click **Refresh** to refresh the table.

Modifying Existing Accounts

Authorized users can modify one of their existing accounts from the Account Management page.

To modify an existing account:

1. Click **Home** in the Main Menu Navigation Bar.
2. Click **Manage Accounts** in the task bar.

   The Account Management page opens.
3. Click the name of the account to be modified.

   The Modify Account page opens.
4. Change the account information as desired, and click **Submit**.

   Note: The User ID is a required field and must be filled in before continuing. If the Change Password at Next Logon? check box is selected, the user is required to change the password when first logging into the system.

   The Enter Password and Select Effective Date | Time page opens.
5. Select an effective date and time for the changes to take affect or select the Schedule Immediately check box.

   See "Effective Date" on page 10 for more information.
6. Click **Submit**.

   The request is submitted and the Account Management page reappears.

To restore the account, see "Restoring Accounts" on page 15.

7. Click **Refresh** to refresh the table.

Suspending or Deprovisioning Accounts

Authorized users can suspend or deprovision their own account from the Account Management page. Suspending an account deactivates the account so the account owner cannot log into the Tivoli Identity Manager system. However, the account is not deleted from the system. Deprovisioning an account deletes the account from the Tivoli Identity Manager system.

To suspend or deprovision an account:

1. Click **Home** in the Main Menu Navigation Bar.
2. Click **Manage Accounts** in the task bar.

   The Account Management page opens.
3. Select the check boxes next to the accounts you want to deprovision or suspend.
4. Click **De-Provision** or click **Suspend**.

   The Deprovision Service(s) page or the Suspend Service(s) page opens, depending on your selection.
5. Select an effective date and time or select the Schedule Immediately check box.

   See "Effective Date" on page 10 for more information.
6. Click **Submit**.

   The request is submitted and the Account Management page reappears.

   To restore the account, see "Restoring Accounts" on page 15.

Restoring Accounts

Authorized users can restore their own suspended account from the Accounts Management page. A new password must be entered, or created, when restoring accounts.

To restore an account:

1. Click **Home** in the Main Menu Navigation Bar.
2. Click **Manage Accounts** in the task bar.

   The Account Management page opens.
3. Select the check boxes next to the accounts you want to restore and click **Restore**.

   Only suspended accounts can be restored.
4. Enter a **New Password**, and confirm it, or select the check box to **Create Password**.

   If you select Create Password, Tivoli Identity Manager generates a password for you and e-mails it to the address associated with the account.
5. Select an effective date and time or select the Schedule Immediately check box.
6. Click **Submit**.

   The request is submitted and the Account Management page reappears.
7. Click **Refresh** to refresh the table.

Changing Passwords

ITIM Users can change the password for their accounts from the Account Management page or the Manage Password page.

By allowing users to manage all of their accounts from one location, users can set the password for more than one account at the same time. However, if the new password does not conform to the password rules for each service, the request fails and the password is not changed. Users should verify that the request is completed successfully before attempting to log into the desired resource using the new password. Users can view the request results on the Completed Requests page. (See "Completed Requests" on page 20 for more information.)

Changing passwords through the Accounts Management page is very similar to changing passwords through the Manage Passwords page. (See "Password Management" on page 11 for more information about the Manage Passwords page.)

To change an account password:

1. Click **Home** in the Main Menu Navigation Bar.
2. Click **Manage Accounts** in the task bar.

   The Account Management page opens.
3. Select the check boxes next to the accounts you want to change the passwords for and click **Change Password**.

   The Account Management Change Password page opens.
4. Type a new password in the New Password Text field and confirm it in the Confirm Password text field **OR** select the Create Password check box.

   If you select Create Password, Tivoli Identity Manager generates a password for you and e-mails it to the address associated with the account.
5. Select an effective date and time **OR** select the Schedule Immediately check box.

   See "Effective Date" on page 10 for more information.
6. Verify that the check boxes next to the accounts for which you want to change the password are selected.
7. Verify that the password conforms to the password rules for the selected services by clicking the View icon next to the services.

   If you are changing the password for more than one service, click the **View Combined Password Rules** link to see a combined list of the restrictive components of each set of password rules.
8. Click **Submit**.

   The request is submitted and the Account Management page reappears.

To Do List

The To Do List page is where ITIM users view and complete actions items that have been assigned to them. These action items can be requests for approval or requests for information. Action items listed in the To Do List are part of workflow processes that cannot be completed properly without a response from the ITIM user.

The To Do List page allows users to approve, reject, abort, or provide information about a request. The To Do List page can also be refreshed to capture and display new action items as they are submitted. Requests for approval or information are typically generated by another user in the system.

Note: Requests that require approval from the requestor are automatically approved. If more than one signature authority is required, only the request sent to

the requestor's own queue is automatically approved. The request must receive approval from additional signature authorities (as required by the workflow design) to complete the request.

The following information is displayed about each action item:

Column Name	Description
Request Id	Transaction number associated with the request.
Action	Type of action requested from the user.
Date Submitted	Date the request is submitted for an action.
Requestee	Name of the user requesting the action.
Subject	Information about the topic of the request.
Status	Current status of the request.

The page can be sorted by the information in each column.

To complete an action item:

1. Click **Home** in the Main Menu Navigation Bar.
2. Click **Access To Do List** in the task bar.

   The To Do List page opens.
3. **OPTIONAL:** Sort the To Do List by the desired field by clicking the arrow next to the field name and selecting the desired attribute.
4. **OPTIONAL:** Display requests of a specific type by selecting the request type from the Type drop-down menu.
5. **OPTIONAL:** Click the View Details icon next to the desired Request ID to view additional information about the desired action item.

   The Request Details page opens.
6. **OPTIONAL:** Click **Cancel** to return to the To Do List Page.
7. Click the link in the Action column for the item to complete.

   The Approve/Reject Request page opens if the item is an Approval/Reject request.
8. Complete one of the following, depending on the type of action item to complete:
   - **Approve/Reject Request**
     a. Select the Approve or Reject radio button.
     b. **Optional:** Type an explanation of the decision in the Explanation text box.
     c. **Optional:** Click the **View Request Data** for information about the request and its settings.
     d. Click **Submit**.

        The response is submitted and the To Do List page reappears.
   - **Provide Information Request**
     a. Provide the requested information.
     b. Click **Submit**.

        The response is submitted and the To Do List page reappears.

Viewing To Do List Request Details

Users can view details about requests in their To Do Lists at any time.

To view details about a pending request:

1. Click **Home** in the Main Navigation Menu Bar.
2. Click **Access To Do List** in the task bar.

   The To Do List page opens.
3. **OPTIONAL:** Sort the request by the desired field by clicking the arrow next to the field name and selecting the desired attribute.

   The To Do List page refreshes with the requests sorted by the selected attribute.
4. Click the View icon next to the request for which you want see the details.

   The Request Details page opens.
5. Select the tab containing the information you wish to see.
6. Click **Cancel** on any tab to return to the To Do List page.

Requests

Request status is available through the View Pending Requests and View Completed Requests icons located in the Home task bar. These sections allow users to view the status of any pending or completed requests. Users are only allowed to view their own requests and results. Administrators can view all requests and results.

The following table lists all valid request types, status, and results that can be found on both the View Completed Requests and View Pending Requests pages.

Request Types	
ALL	All
AA	Account Add
	Account Add Operation
AC	Account Change
	Account Change Operation
AP	Account Password Change
DA	Add Dynamic Role
PA	Add Provisioning Policy
SA	Add Service Selection Policy
	Authorize Provision
LP	Change Password for Multiple Accounts
	Custom Operation
AD	Delete Account
	Delete Business Unit
LD	Delete Multiple Accounts
	Delete Organization
PD	Delete Provisioning Policy
SD	Delete Service Selection Policy
UD	Delete User

MD	Delete Users
	Enforce Policy for Accounts
	Enforce Policy for User
	Enforce Policy for Users
	Entitlement Process
DC	Modify Dynamic Role
PC	Modify Provisioning Policy
SC	Modify Service Selection Policy
UA	New User
	Policy enforcement action changed
	Provision Ordered Accounts
RC	Reconciliation
DD	Remove Dynamic Role
AR	Restore Account
	Restore Business Unit
LR	Restore Multiple Accounts
	Restore Organization
UR	Restore User
MR	Restore Users
	Self Registration
AS	Suspend Account
	Suspend Business Unit
LS	Suspend Multiple Accounts
	Suspend Organization
US	Suspend User
MS	Suspend Users
UO	User BU Change
UC	User Data Change
	User Role Change
Request States	
	Aborted
	Bypassed
	Completed
	Not Started
	Running
	Suspended
	Terminated
Request Results	
	Approved
	Escalated
	Failed
	Participant Resolution Failed

	Pending
	Rejected
	Skipped
	Submitted
	Success
	Timeout
	Warning

Pending Requests

The Pending Requests page is where ITIM users view requests that have been submitted to the Tivoli Identity Manager system but have not been completed within the system. When viewing the Pending Requests page, users should click **Refresh** periodically to capture and view new requests that are submitted and existing requests that have been completed.

Pending requests can be sorted by:

- Request Id
- Date Submitted
- Type
- Requestor
- Requestee
- Subject
- Status

Completed Requests

The Completed Requests page displays all requests that have been completed that day. Users can sort the page by each column's information by clicking the arrows at the top of each column. To view details about each request, click the View icon next to the Request ID at the left side of the page.

Note: To refine the information that is displayed by Tivoli Identity Manager, use the Filter Requests selection. The Filter Requests selection allows users to filter the information shown by Date, Requestor, Requestee, or Type of request.

To reach the Completed Requests page:

1. Click **Home** in the Main Menu Navigation Bar.
2. Click **View Completed Requests**.

Transaction Audits

Tivoli Identity Manager allows you to identify requestors of transaction data. Each user needs to be uniquely identified in audit records by assigning each of them a unique key for the Tivoli Identity Manager person class. To do this, you must assign unique keys by accessing the data store used by your directory server software and configure it to supply unique keys for each member contained within the **cn** data store.

The Name field listed for a completed request can be configured through the Entities Tab located under System Configuration. The default configuration of the Name attribute setting is the **cn** (common name) of the person.

Personal Information

The Personal Information section contains information about you, as the owner of accounts managed by Tivoli Identity Manager.

The Personal Information form can be customized by a system administrator. The default Personal Information form has the following items listed:

Tab	Field	Description
Personal Information	Last Name	Account owner's last name.
	Full Name	Account owner's full name. Used to identify account owner in a list of people.
	First Name	Account owner's first name.
	Initials	Account owner's initials.
	Home Address	Account owner's home address.
	Shared Secret	Password used by account owner to retrieve password for a new account. This is a required value if the Tivoli Identity Manager Server system generates the initial password for the account.
	Organizational Roles	Organizational roles to which the account owner belongs.
Corporate Information	Room Number	Account owner's seat location number (typically, from a corporate seating chart).
	Employee Number	Account owner's employee number.
	Title	Account owner's job title.
	Supervisor	Account owner's direct supervisor.
	Postal Address	Account owner's corporate address.
	Secretary	Name of account owner's secretary (if applicable).
Communications Information	Email Address	Account owner's e-mail address (typically, the account owner's first initial and last name). Used by the system to notify account owner of requests and other actions.
	Telephone Number	Account owner's office number.
	Mobile Phone Number	Account owner's corporate cellular phone number.
	Pager	Account owner's corporate pager number.
	Home Phone	Account owner's home phone number.
	Aliases	Additional aliases used by the account owner. This attribute is used by Tivoli Identity Manager to match your account's User IDs on managed resources.

To enter personal information:

1. Click **Home** in the Main Menu Navigation Bar.
2. Click **Access Personal Information** in the task bar.

   The Access Personal Information page opens.
3. Modify the information on the Personal Information tab, Corporate Information tab, and Communications Information tab as desired.
4. Click **Submit**.

   Note: Organizational Roles can be added on the Personal Information page, which confers access to any Managed Resources allowed by membership in an Organizational Role.

Delegating Authority

You use the Delegate Authority page to designate individuals to whom your approval authority is delegated. This is used in request approval and to provide information as a step in request provisioning.

You can select more than one delegate, but never more than one for the same date period. If you want to change the individual delegated for a time period, you must delete the original delegate and add a new one for the selected time period.

Note: Be aware of the potential implications of providing someone other than yourself the ability to perform actions on your behalf. You are responsible for all delegation decisions authorized as a result of your delegation.

Adding a Delegate

To delegate authority:

1. Click **Home** in the Main Menu Navigation Bar.
2. Click **Delegate Authority** in the task bar.

   The Delegate Authority page opens.
3. Click **Add**.
4. Locate an individual using the Search feature, and then select the check box next to the individual's name and click **Add**.
5. Select a beginning and ending date for your approval authority being delegated.
6. Click **Submit**.

Changing the Delegate

To change the delegate for a time period:

1. Click **Home** in the Main Menu Navigation Bar.
2. Click **Delegate Authority** in the task bar.
3. Select the check box next to the name of the existing delegate and click **Delete**.

   The Confirm Deletion page opens.
4. Click **Submit**.

   The delegate is removed from the delegate list.
5. Use the Adding a Delegate procedure to add a new delegate for the time period.

Modifying the Selected Delegate

To change the time period for an existing delegate:

1. Click **Home** in the Main Menu Navigation Bar.
2. Click **Delegate Authority** in the task bar.
3. Click the delegate's name you want to change.
4. Make any changes to the From/To dates.
5. Click **Submit**.

Password Challenge/Response Answers

ITIM users can modify their Password Challenge/Response answers at any time. If there is more than one Password Challenge/Response question to provide answers for, one answer can be changed without modifying the other answers.

By default, this feature is disabled. If this option is selected and the feature is disabled, a message appears on the page stating that this feature is currently disabled. However, if this feature is enabled, the following procedures can be used to modify password challenge/response answers.

To modify password challenge/response answers:

1. Click **Home** in the Main Menu Navigation Bar.
2. Click **Password Challenge Response** in the task bar.

   The Challenge Response page opens.
3. Modify the answer to the desired challenge/response questions and click **Submit**.

   The changes to the challenges/response answers are saved.

Chapter 5. Reports

An authorized user can use the Tivoli Identity Manager report system to generate reports. Reports organize system activity information according to specific criteria and display the results in a specific visual format. All reports are rendered in a PDF file format.

Tivoli Identity Manager provides two types of reports:

- Pre-defined, or standard, reports

  There are seven standard report types that are provided by the Tivoli Identity Manager product. These reports are pre-defined and cannot be modified.
- User-defined, or custom, reports

  Custom report templates are designed using a report designer and then imported into the Tivoli Identity Manager environment, where they appear in the Reports menu of the Tivoli Identity Manager GUI. You can use the built-in Report Designer or a third-party report designer, such as the Crystal Reports Designer.

Important: Adobe Acrobat Reader™ is required to view reports. You must also have Internet Explorer version 5.5 with service pack 2 or later or Netscape version 4.75.

Every user who has an ITIM account can view reports. However, the user's ITIM group must be granted access to a specified report using a report ACI. Users can also see any custom reports that they are given rights to view. The reports available to various users can be limited by setting specific report ACIs to explicitly grant or deny access to specific types of reports.

End users can see only a report of the activity that is specific to the end user, either as the requestee or the requestor. For example, managers can view reports for requests they initiated or requests that are made for them. But, employees with no supervisory or managerial position only view reports only for requests that are made for them because they cannot initiate a request.

© Copyright IBM Corp. 2004

Report Types

The following table describes the types of reports available in Tivoli Identity Manager. However, the reports available to a specific user depend on the users ITIM group membership.

Report Type	Description
Operation	Pre-defined (standard) report. Lists Tivoli Identity Manager operation requests by type of operation, date, who requested the operation, and for whom the operation is requested. You can define the following parameters for this report: • Requestor • Requestee • Operations • Start Date • End Date
Service	Pre-defined (standard) report. Lists existing service instances by date, who requested the operation, and for whom the operation is requested. You can define the following parameters for this report: • Requestor • Requestee • Service Instance • Start Date • End Date
User	Pre-defined (standard) report. Lists all Tivoli Identity Manager operations by date, who requested the operation, and who the operation is requested for. You can define the following parameters for this report: • Requestor • Requestee • Start Date • End Date
Rejected	Pre-defined (standard) report. Lists requests denied by date, who requested the operation, and who the operation is requested for. You can define the following parameters for this report: • Requestor • Requestee • Start Date • End Date

Report Type	Description
Reconciliation	Pre-defined (standard) report. Lists the orphan accounts found since the last reconciliation was performed. You can define the following parameters for this report: • Service Instance
Dormant	Pre-defined (standard) report. Lists services with no activity within number of days selected. You can define the following parameters for this report: • Service Instance • Number of days service has been dormant
Account	Pre-defined (standard) report. Lists people and their associated accounts and whether or not the account is in compliance with current policies. You can define the following parameters for this report: • Service Instance • Business Unit
Custom	User-defined report. User-defined report templates designed using a report designer and then imported into the Tivoli Identity Manager environment.

The following list includes all the reports that can be run on a specific service instance:

- Service
- Reconciliation
- Dormant
- Account
- Custom

The following sections describe, in detail, the various report types.

Operation Report

The Operation Report shows which Tivoli Identity Manager operations were requested, who requested them, and for whom the operations were requested. The report can show requests for a specific operation for all system users or for one specific system user. You can then ask the report to show all users the operation was requested to be performed upon, or select only one user and view requests for the selected operation to be performed. You can also enter a date range and only operation requests that fall within that range will be shown.

The following table describes the search fields reports can be limited to:

Requestor	The requestor is the user who initiated the request. If a requestor is not selected, Tivoli Identity Manager searches all requests initiated by any system user.

Requestee	The requestee is the user being added, modified, or deleted. If a requestee is not selected, Tivoli Identity Manager searches all requests for any person entity.
Operation	The type of operation Tivoli Identity Manager searches for when generating the report. **Required**. Types of operations available: • Account Add • Account Change • Account Password Change • Add Dynamic Role • Add Provisioning Policy • Add Service Selection Policy • Change Password for Multiple Accounts • Delete Multiple Accounts • Delete Account • Delete Provisioning Policy • Delete Service Selection Policy • Delete User • Delete Users • Modify Dynamic Role • Modify Provisioning Policy • Modify Service Selection Policy • New User • Reconciliation • Remove Dynamic Role • Restore Account • Restore Multiple Accounts • Restore User • Restore Users • Suspend Account • Suspend Multiple Accounts • Suspend User • Suspend Users • User BU Change • User Data Change
Start / End Date and Time	Time and date range that the report is limited to. Only service instances that are active within the date/time range selected are included on the report.

To generate an Operation Report:

1. Click **Report** in the Main Menu Navigation Bar.
2. Click **Run Report** in the task bar.
   The Reports Menu page opens.
3. Click **Operation Report**.
   The Operation Report Search page opens.
4. **OPTIONAL:** Select a requestor.

a. Click **...get Identity Manager User**.

   The User Search page opens.

b. Select a search attribute from the Select an Attribute menu.

c. Select a search filter from the Select an Expression menu.

d. Type a search parameter in the text field, and click **Search**.

   The Search Filter Results page opens.

e. Select the radio button next to the desired user and click **Add**.

   The Operation Report Search page reappears with the selected requestor listed in the Requestor field.

5. **OPTIONAL:** Select a requestee.

   a. Click **...get a Person**.

      The User Search page opens.

   b. Select a person class from the Select Type of Person menu if more than one type of Person exists.

   c. Select a search attribute from the Select an Attribute menu.

   d. Select a search filter from the Select an Expression menu.

   e. Type a search parameter in the text field, and click **Search**.

      The Search Filter Results page opens.

   f. Select the radio button next to the desired person and click **Add**.

      The Operation Report Search page reappears with the selected requestee listed in the Requestee field.

6. Select an operation type from the Operations menu.

7. Select start and end dates and times by selecting the month, day, year, and time from the respective menus.

8. Click **Submit**.

   A report is generated based on the selected search criteria selected. The report is displayed using Adobe Acrobat Reader.

9. To save the report in PDF format to the client machine, click on the **Save** icon in the report window toolbar. In some situations, the default file name that displays in the File Name field may be an invalid file name (too many characters). Browse to the directory where you want to save this file and re-enter a valid file name in the File Name field. Click **Save**.

Service Report

The Service Report lists requests for an existing service instance. Only requests of the service instances requested by the selected system user (or ALL system users), and requested for the selected person (or ALL persons), that fall within the Date/Time Range, will be shown on the report.

The following table describes the search fields that reports can be limited to:

Requestor	The requestor is the user who initiated the request. If a requestor is not selected, Tivoli Identity Manager searches all requests initiated by any system user.
Requestee	The requestee is the user being added, modified, or deleted. If a requestee is not selected, Tivoli Identity Manager searches all requests for any person entity.
Service Instance	**Required.** A service instance is a service available in Tivoli Identity Manager or an individual instance of a service, if the service has multiple instances.

Start / End Date and Time	Time and date range that the report is limited to. Only requests submitted within the date/time range selected are included on the report.

To generate a Service Report:

1. Click **Report** in the Main Menu Navigation Bar.
2. Click **Run Report** in the task bar.

   The Reports Menu page opens.
3. Click **Service Report**.

   The Service Report search page opens.
4. **OPTIONAL:** Select a requestor.
   a. Click **...get Identity Manager User**.

      The User Search page opens.
   b. Select a search attribute from the Select an Attribute menu.
   c. Select a search filter from the Select an Expression menu.
   d. Type a search parameter in the text field, and click **Search**.

      The Search Filter Results page opens.
   e. Select the radio button next to the desired user and click **Add**.

      The Service Report Search page reappears with the selected requestor listed in the Requestor field.
5. **OPTIONAL:** Select a requestee.
   a. Click **...get a Person**.

      The User Search page opens.
   b. Select a search attribute from the Select an Attribute menu.
   c. Select a search filter from the Select an Expression menu.
   d. Type a search parameter in the text field, and click **Search**.

      The Search Filter Results page opens.
   e. Select the radio button next to the desired individual and click **Add**.

      The Service Report Search page reappears with the selected requestee listed in the Requestee field.
6. Select a service instance.
   a. Click **...get a Service**.

      The Service Search page opens.
   b. Select a service profile from the Select Type of Service menu.
   c. Select a search attribute from the Select an Attribute menu.
   d. Select a search filter from the Select an Expression menu.
   e. Type a search parameter in the text field, and click **Search**.

      The Search Filter Results page opens.
   f. Select the radio button next to the desired service and click **Add**.

      The Service Report Search page reappears with the selected service listed in the Service Instance field.
7. Select start and end dates and times by selecting the month, day, year, and time from the respective menus.
8. Click **Submit**.

   A report is generated based on the selected search criteria selected. The report is displayed using Adobe Acrobat Reader.

9. To save the report in PDF format to the client machine, click on the **Save** icon in the report window toolbar. In some situations, the default file name that displays in the File Name field may be an invalid file name (too many characters). Browse to the directory where you want to save this file and re-enter a valid file name in the File Name field. Click **Save**.

User Report

The User Report lists all Tivoli Identity Manager operations that were requested, who requested them, and upon whom the operations were requested to act. You can choose to show requests for all system users or for one specific system user. You can then ask the report to show all people the requests were to be performed upon, or select only one person and view all requests for that person from all system users or from one selected system user. You can also enter a date range and only operation requests that fall within that range will be shown.

The following table describes the search fields reports can be limited to.

Requestor	The requestor is the user who initiated the request. If a requestor is not selected, Tivoli Identity Manager searches all requests initiated by any system user.
Requestee	The requestee is the user being added, modified, or deleted. If a requestee is not selected, Tivoli Identity Manager searches all requests for any person entity.
Start / End Date and Time	Time and date range the report is limited. Only service instances that are active within the date/time range selected are included on the report.

To generate a User Report:

1. Click **Report** in the Main Menu Navigation Bar.
2. Click **Run Report** in the task bar.

   The Reports Menu page opens.
3. Click **User Report**.

   The User Report Search page opens.
4. **OPTIONAL:** Select a requestor.
   a. Click **...get Identity Manager User**.

      The User Search page opens.
   b. Select a search attribute from the Select an Attribute menu.
   c. Select a search filter from the Select an Expression menu.
   d. Type a search parameter in the text field, and click **Search**.

      The Search Filter Results page opens.
   e. Select the radio button next to the desired user and click **Add**.

      The User Report Search page reappears with the selected requestor listed in the Requestor field.
5. **OPTIONAL:** Select a requestee.
   a. Click **...get a Person**.

      The User Search page opens.
   b. Select a search attribute from the Select an Attribute menu.
   c. Select a search filter from the Select an Expression menu.
   d. Type a search parameter in the text field, and click **Search**.

The Search Filter Results page opens.

e. Select the radio button next to the desired person and click **Add**.

The User Report Search page reappears with the selected requestee listed in the Requestee field.

6. Select start and end dates and times by selecting the month, day, year, and time from the respective menus.
7. Click **Submit**.

A report is generated based on the selected search criteria selected. The report is displayed using Adobe Acrobat Reader.

8. To save the report in PDF format to the client machine, click on the **Save** icon in the report window toolbar. In some situations, the default file name that displays in the File Name field may be an invalid file name (too many characters). Browse to the directory where you want to save this file and re-enter a valid file name in the File Name field. Click **Save**.

Rejected Report

The Rejected Report lists all Tivoli Identity Manager requests that were rejected. You can choose to see all rejected operations, or select specific system users to see only the operations that were rejected for the selected system user. You can also choose to see only operations that were rejected for a specific person the operation was to be performed upon. In either case, all Tivoli Identity Manager operations that meet the requestor/requestee criteria, regardless of the type of operation, are displayed on the report.

The following table describes the search fields that reports can be limited to:

Requestor	The requestor is the user who initiated the request. If a requestor is not selected, Tivoli Identity Manager searches all requests initiated by any system user
Requestee	The requestee is the user being added, modified, or deleted. If a requestee is not selected, Tivoli Identity Manager searches all requests for any person entity.
Start / End Date and Time	Time and date range the report is limited. Only service instances that are active within the date/time range selected are included on the report.

To generate a Rejected Report:

1. Click **Report** in the Main Menu Navigation Bar.
2. Click **Run Report** in the task bar.

The Reports Menu page opens.

3. Click **Rejected Report**.

The Rejected Report Search page opens.

4. **OPTIONAL:** Select a requestor.
   a. Click **...get Identity Manager User**.

   The User Search page opens.

   b. Select a search attribute from the Select an Attribute menu.
   c. Select a search filter from the Select an Expression menu.
   d. Type a search parameter in the text field, and click **Search**.

   The Search Filter Results page opens.

   e. Select the radio button next to the desired user and click **Add**.

The Rejected Report Search page reappears with the selected requestor listed in the Requestor field.

5. **OPTIONAL:** Select a requestee.
   a. Click **...get a Person**.
      The User Search page opens.
   b. Select a search attribute from the Select an Attribute menu.
   c. Select a search filter from the Select an Expression menu.
   d. Type a search parameter in the text field, and click **Search**.
      The Search Filter Results page opens.
   e. Select the radio button next to the desired person and click **Add**.
      The Rejected Report Search page reappears with the selected requestee listed in the Requestee field.
6. Select start and end dates and times by selecting the month, day, year, and time from the respective menus.
7. Click **Submit**.
   A report is generated based on the selected search criteria selected. The report is displayed using Adobe Acrobat Reader.
8. To save the report in PDF format to the client machine, click on the **Save** icon in the report window toolbar. In some situations, the default file name that displays in the File Name field may be an invalid file name (too many characters). Browse to the directory where you want to save this file and re-enter a valid file name in the File Name field. Click **Save**.

Reconciliation Report

The Reconciliation Report lists the following information:

- Number of orphan accounts created
- Number of owned accounts created
- Number of accounts updated
- Number of local accounts removed
- Total number of accounts processed
- Detailed listing of person and account entities that were changed

To generate a Reconciliation Report:

1. Click **Report** in the Main Menu Navigation Bar.
2. Click **Run Report** in the task bar.
   The Reports Menu page opens.
3. Click **Reconciliation Report**.
   The Reconciliation Report search page opens.
4. Select a service instance.
   a. Click **...get a Service**.
      The Service Search page opens.
   b. Select a service profile from the Select Type of Service menu.
   c. Select a search attribute from the Select an Attribute menu.
   d. Select a search filter from the Select an Expression menu.
   e. Type a search parameter in the text field, and click **Search**.
      The Search Filter Results page opens.
   f. Select the radio button next to the desired service and click **Add**.

The Reconciliation Report Search page reappears with the selected service listed in the Service Instance field.

5. Click **Submit**.

   A report is generated based on the selected search criteria selected. The report is displayed using Adobe Acrobat Reader.

6. To save the report in PDF format to the client machine, click on the **Save** icon in the report window toolbar. In some situations, the default file name that displays in the File Name field may be an invalid file name (too many characters). Browse to the directory where you want to save this file and re-enter a valid file name in the File Name field. Click **Save**.

Dormant Report

The Dormant Report lists all accounts for the specified service that have not been used within a defined number days and accounts that have never been used.

The following table describes the search fields reports can be limited to.

Service Instance	**Required.** A service instance is a service available in Tivoli Identity Manager or an individual instance of a service, if the service has multiple instances.
Has Been Dormant for No. of Days	**Required.** Number of days an account on the selected service has been dormant.

To generate a Dormant Report:

1. Click **Report** in the Main Menu Navigation Bar.
2. Click **Run Report** in the task bar.

   The Reports Menu page opens.

3. Click **Dormant Report**.

   The Dormant Report search page opens.

4. Select a service instance.
   a. Click **...get a Service**.

      The Service Search page opens.

   b. Select a service profile from the Select Type of Service menu.
   c. Select a search attribute from the Select an Attribute menu.
   d. Select a search filter from the Select an Expression menu.
   e. Type a search parameter in the text field, and click **Search**.

      The Search Filter Results page opens.

   f. Select the radio button next to the desired service and click **Add**.

      The Dormant Report Search page reappears with the selected service listed in the Service Instance field.

5. Type the number of dormant days to search for in the Has Been Dormant for No of Days text field.
6. Click **Submit**.

   A report is generated based on the selected search criteria selected. The report is displayed using Adobe Acrobat Reader.

7. To save the report in PDF format to the client machine, click on the **Save** icon in the report window toolbar. In some situations, the default file name that displays in the File Name field may be an invalid file name (too many

characters). Browse to the directory where you want to save this file and re-enter a valid file name in the File Name field. Click **Save**.

Account Reports

The Account Report lists individuals and their associated accounts and whether or not the account is in compliance with current policies for the specified business unit and its sub-units.

The following table describes the search fields reports can be limited to.

Service Instance	**Required.** A service instance is a service available in Tivoli Identity Manager or an individual instance of a service, if the service has multiple instances.
Business Unit	**Required.** The Business Unit is the specific unit for which to list the users and their associated accounts. The types of business unit that can be specified are: • Admin Domain • Business Person Organization • Location • Organization • Organizational Unit

To generate an Account Report:

1. Click **Report** in the Main Menu Navigation Bar.
2. Click **Run Report** in the task bar.
   The Reports Menu page opens.
3. Click **Account Report**.
   The Account Report search page opens.
4. Select a service instance.
   a. Click **...get a Service**.
      The Service Search page opens.
   b. Select a service profile from the Select Type of Service menu.
   c. Select a search attribute from the Select an Attribute menu.
   d. Select a search filter from the Select an Expression menu.
   e. Type a search parameter in the text field, and click **Search**.
      The Search Filter Results page opens.
   f. Select the radio button next to the desired service and click **Add**.
      The Account Report Search page reappears with the selected service listed in the Service Instance field.
5. Select a Business Unit.
   a. Click **...get a Business Unit**.
      The Search page opens.
   b. Select a type of business unit from the Select a type menu.
   c. Select a search attribute from the Select an Attribute menu.
   d. Select an expression from the Select an Expression menu.
   e. Type a search parameter in the text field, and click **Search**.
      The Search Filter Results page opens.
   f. Select the radio button next to the desired service and click **Continue**.

The account report Search page reappears with the selected business unit listed in the Business Unit field.

6. Click **Submit**.

   A report is generated based on the selected search criteria selected. The report is displayed using Adobe Acrobat Reader.

7. To save the report in PDF format to the client machine, click on the **Save** icon in the report window toolbar. In some situations, the default file name that displays in the File Name field may be an invalid file name (too many characters). Browse to the directory where you want to save this file and re-enter a valid file name in the File Name field. Click **Save**.

Custom Reports

Custom report templates are created using the built-in Report Designer or imported from a third-party report designer (such as Crystal Reports). Custom reports appear listed with the standard reports in the Reports menu of the Tivoli Identity Manager GUI.

System administrators can customize reports for an organization's needs. Display fields contained in custom reports will vary depending upon the construction of the report template.

To generate and save a Custom Report:

1. Click **Report** in the Main Menu Navigation Bar.
2. Click **Run Report** in the task bar.

   The Reports Menu page opens.

3. Select the custom report from the list.
4. Specify the report format (PDF/CSV).

   Note: This option appears for reports designed using the Tivoli Identity Manager custom reporting interface.

5. Enter input required to generate the report, if applicable.

   Note: For custom reports built with the Tivoli Identity Manager Report Designer, user input should adhere to syntax rules similar to those for an SQL query. For example, to get all person names starting with J, the user input will be J% and not J*.

   Note: For Crystal reports, user input should adhere to standard regular expression syntax. For example, to get all person names starting with **J**, the user input will be **J***.

6. Click **Submit**.

   A report is generated and displayed in the format chosen.

7. To save the custom report in PDF/CSV format to the client machine, click on the **Save** icon in the report window toolbar. If the **Save** icon is not visible in the toolbar, use the option in the window menubar to save the report. In some situations, the default file name that displays in the File Name field may be an invalid file name (too many characters). Browse to the directory where you want to save this file and re-enter a valid file name in the File Name field. Click **Save**.

   To save a Crystal report in any supported format to the client machine, export the Crystal report using the **Export** option in the report output page. Then select the output format from the list and **Save** the report.

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

© Copyright IBM Corp. 2004

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged should contact:

IBM Corporation
2ZA4/101
11400 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Trademarks

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

AIX
DB2
IBM
IBM logo
OS/390
SecureWay
Tivoli
Tivoli logo
Universal Database
WebSphere
z/OS
zSeries

Lotus® is a registered trademark of Lotus Development Corporation and/or IBM Corporation.

Domino™ is a trademark of International Business Machines Corporation and Lotus Development Corporation in the United States, other countries, or both.

Microsoft®, Windows®, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

UNIX® is a registered trademark of The Open Group in the United States and other countries.

	Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Glossary

A

access. The privilege to use information or data stored on computer systems.

account. The set of parameters that define the login information and access control information for a user.

account report. A report that lists people and their associated accounts and whether or not the account is in compliance with current policies.

active account. An account that exists and that is in use by the owner to access a resource.

alias. An identity for a user, usually referred to as the user ID. A person can have several aliases, for example: GSmith and GWSmith.

audit trail. The record of transactions for a computer system during a given time period.

authentication. The process of identifying an individual, usually based on a user name and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects basedon their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

authorization. In computer security, the right granted to a user to communicate with or make use of a computer system. The process of granting a user either complete or restricted access to an object, resource, or function.

Most computer security systems are based on a two-step process. The first stage is authentication, which ensures that a user is who he or she claims to be. The second stage is authorization, which allows the user access to various resources based on the user's identity.

B

branch. Each level within the organization tree is called a branch. Each type of branch in the tree is indicated by a different icon. The contents of a branch with sub-units can be viewed by clicking the plus (+) sign next to it.

business partner organization. One of the types of subsidiary entities that can be added to an organization. Typically, a business partner organization is used to identify a contractor, supplier, or other groups of individuals who are not direct employees but may need access to a company's resources.

business partner person. A person in a business partner organization.

business unit. A subsidiary entity of an organization.

C

challenge response. An authentication method that requires users to respond to a prompt by providing private information to verify their identity when logging in to the network.

completed requests. Requests that were submitted to the system and that are completed.

credential. The User ID and password information for a user, which allows access to an account.

D

delegate. An individual who is designated as the responsible party to approve requests or provide information for requests for another user.

domain administrator. An administrator that can define and manage provisioning entities, policies, services, workflow definitions, roles, and users within their admin domain, but only in his or her own admin domain.

E

entity. 1) A person or object for which information is stored.

2) One of the following classes, as referred to by the Tivoli Identity Manager system:

- Person
- BPPerson
- Organization
- BPOrganization

escalation participant. In identity management, a person that has the authority to respond to requests that participants do not respond to within a specified escalation time. An escalation participant can be identified as an individual, as a roles, or by using a custom JavaScript script.

escalation limit. The amount of time, in days, hours, minutes or seconds, that a participant has to respond to a request, before an escalation occurs.

© Copyright IBM Corp. 2004

I

identity policy. The rules by which the Tivoli Identity Manager system defines how a user's ID is created.

inactive account. An account that exists in the system, but that is not in use by the account owner.

L

location. One of the types of subsidiary entities that can be added to an organization. Typically, locations are used to logically separate geographic locations for organizational management purposes.

O

operation report. A report that lists Tivoli Identity Manager operation requests by type of operation, date, who requested the operation, and who the operation is requested for.

organization. In identity management, a body of users and resources which is fairly independent. Although the sharing of resources between organizations is possible, the level of integration between the organizations is relatively low. Generally, an organization represents a company.

organization tree. A hierarchical structure of the organization that provides a logical place to create, access, and store organizational information.

organizational unit. A body of users and resources within an organization defined to sub-divide an organization into more manageable groups. Users are assigned to only one organizational unit. Resources are also assigned to only one organizational unit unless they are defined as global to an organization.

owner. A person in the Tivoli Identity Manager system that owns an account or a service.

P

participant. In identity management, a person that has the authority to respond to a request that is submitted through the workflow engine. A participant can be identified as an individual, as a roles, or by using a custom JavaScript script.

password. In computer and network security, a specific string of characters entered by a user and authenticated by the system, which allows the user to gain access to the system and to the information stored within it.

password expiration period. The amount of time a password can be used before the user is forced to change it.

password policy. The rules that define the set parameters that all passwords must meet, such as length, and the type of characters allowed and disallowed.

pending requests. Requests that have been submitted to the system but that have not yet been completed.

personal information. A user's personal information. This information can include last name, first name, home address, phone number, e-mail address, office number, supervisor, and so on.

policy. In Tivoli, a set of rules that are applied to managed resources. For example, a policy can apply to passwords or to resources that a user attempts to access.

policy enforcement. The manner in which the Tivoli Identity Manager system allows or disallows accounts that violate provisioning policies.

R

reconciliation. The process of comparing the information the central data repository to the managed agent system and identifying the discrepancies between the two.

reconciliation report. A report that lists the orphan accounts found since the last reconciliation was performed.

rejected report. A report that lists requests denied by date, who requested the operation, and who the operation is requested for.

request. An action item in the Tivoli Identity Manager system asking for approval or information.

requestee. The person for whom a request is submitted.

requestor. A person who submits a request.

resource. A hardware, software, or data entity that is managed by Tivoli software. See also managed resource.

restore. To reactivate an account that was suspended.

request for information (RFI). In identity management, an action item that requests additional information from the specified participant and that is a required step in the workflow.

S

shared secret. An encrypted value used to retrieve a user's initial password to access the Tivoli Identity Manager system. This value is defined when the user's personal information is initially loaded into the system.

supervisor. A person in the Tivoli Identity Manager system that is designated as the owner of a business unit.

suspend. The act of deactivating an account so the account owner cannot log into the resource.

T

to do list. The list of actions items assigned to a user for completion.

U

user. Any person who interacts with the system.

user interface (UI). The display used by the user to interact with the system.

user name. The ID used by the user to access the system. This ID also identifies the user to the system and allows the system to determine the user's access rights based on the user's membership in various organizational roles and ITIM groups.

user report. A report that lists all Tivoli Identity Manager operations by date, who requested the operation, and who the operation is requested for.

Index

A

account
  report
    description 27
account report
  description 35
  generating 35
accounts
  adding 14
  deprovisioning 15
  managing 13
  modifying 14
  restoring 15
  retrieving password 5
  suspending 15
audience v

C

Completed Requests
  description 20
  viewing 20
custom
  report
    description 27
custom report
  description 36
  generating 36

D

delegate authority
  adding 22
  changing 22
  description 22
documents
  accessing online vi
dormant
  report
    description 27
dormant report
  description 34
  generating 34

E

effective date 10
employee
  contact information
    aliases 21
    cellular phone number 21
    e-mail address 21
    home phone number 21
    office phone number 21
    pager number 21
  corporate information 21
    number 21
    postal address 21
    room number 21
employee *(continued)*
  corporate information *(continued)*
    secretary 21
    supervisor 21
    title 21
  personal information
    first name 21
    full name 21
    home address 21
    initials 21
    last name 21
    organizational roles 21
    shared secret 21

G

general features
  effective date 10
  navigation
    Main Menu Navigation Bar 9
    methods 9
    task bar 9
  online help 10

H

Home
  account management
    adding new accounts 14
    deprovisioning accounts 15
    description 13
    modifying existing accounts 14
    restoring accounts 15
    suspending accounts 15
  changing passwords 15
  completed requests
    description 20
  delegating authority
    adding a delegate 22
    changing a delegate 22
    description 22
    modifying a delegate 23
  functional areas 11
  password
    management 11
    modifying Challenge/Response answers 23
  pending requests
    description 20
  personal information
    description 21
  To Do List
    description 16
    viewing request details 18

L

login
  forgotten password 6
  routine 5
logout
  routine 7

M

main menu navigation bar 9
managing
  accounts 13
  password 11

N

navigation
  main menu navigation bar 9
  methods 9
  taskbar 9

O

online help 10
operation report
  description 26, 27
  generating 28

P

password
  Challenge/Response
    answers 6, 23
    purpose 6
  forgotten
    configuring Challenge/Response answers 23
    logging in 6
  managing 11
Pending Requests
  description 20
Personal Information 21
  adding 22
  Communications Information tab
    Aliases 21
    Email Address 21
    Home Phone 21
    Mobile Phone Number 21
    Pager 21
    Telephone Number 21
  Corporate Information tab
    Employee Number 21
    Postal Address 21
    Room Number 21
    Secretary 21
    Supervisor 21
    Title 21
  modifying 22
  Personal Information tab
    First Name 21
    Full Name 21
    Home Address 21
    Initials 21

© Copyright IBM Corp. 2004

Personal Information *(continued)*
Personal Information tab *(continued)*
Last Name 21
Organizational Roles 21
Shared Secret 21
policy enforcement
compliancy flag
compliant 13
noncompliant 13
question mark 13
warning 13
publications
accessing online vi

R

reconciliation
report
description 27, 33
generating 33
rejected
report
description 26
rejected report
description 32
generating 32
report
account
description 27, 35
generating 35
custom
description 27, 36
generating 36
dormant
description 27, 34
generating 34
operation
description 26, 27
generating 28
reconciliation
description 27, 33
generating 33
rejected
description 26, 32
generating 32
service
description 26, 29
generating 30
types
account 27, 35
custom 27, 36
dormant 27, 34
operation 26, 27
reconciliation 27, 33
rejected 26, 32
service 26, 29
user 26, 31
user
description 26, 31
generating 31

S

service
report
description 26, 29
service *(continued)*
report *(continued)*
generating 30
shared secret 21

T

taskbar 9
To Do List
description 16
sorting 18
viewing details 18

U

user
report
description 26, 31
generating 31
user interface
navigation
Main Menu Navigation Bar 9
task bar 9

Program Number: 5724-C34

Printed in USA

SC32-1152-02